4半期レポート（2008年4月-2008年6月）

APWG Phishing Activity Trends Report (Q2/2008)
日本語版

2008 年 12 月 20 日

目次

1. APWG Phishing Activity Trends Report 2008年第2四半期　日本語版

・レポートの調査範囲

『APWG Phishing Activity Trends Report』では、APWGがウェブサイトhttp://www.antiphishing.org上あるいはAPWGグループ宛ての次の電子メールreportphishing@antiphishing.orgにて報告を受けたフィッシング攻撃の事例を分析しています。またAPWGは、会員企業によるCrimeware（クライムウェア）の傾向（タイプ、発生数、拡散の仕方）について調査した結果をまとめています。Crimeware（クライムウェア）についてはこのレポートの後半でまとめています。

・フィッシング（phishing）の定義

『フィッシング(phishing)』とはオンライン上での個人情報の窃盗行為のことを指し、ソーシャルエンジニアリングや悪意のあるプログラムを使い、被害者のクレジットカード番号や口座のユーザーネーム・パスワード、社会保障番号等を巧みに暴き出すものです。ソーシャルエンジニアリングでは偽装した電子メールが使われ、受信者を騙して、ユーザーネームやパスワードなどの情報を盗むために用意した偽装ウェブサイトへ誘導します。社会的信用が確立している大手の銀行やオンライン小売業者、クレジットカード会社の商標を乗っ取ることにより、フィッシング犯は被害者を信用させ、個人情報を盗み出すことに成功しています。また、悪意のあるプログラム（Crimeware：クライムウェア）をPCに仕掛けて個人情報を盗む場合には、キーロガーがしばしば使用されています。さらに、インターネット接続時に経由するルートを不正に改ざんし、偽装ウェブサイトへ誘導するような手法もあります。

・レポートの要約

APWGへ届けられたユニークなフィッシング攻撃は本四半期中を通して13%上昇し、6月に28,151件に達しました。

6月にAPWGへ届けられたユニークなフィッシングサイトは、4月より9%以上減少し18,509件になりました。

5月は、悪用された商標が294件で最高記録を出し、四半期を通して見た485件の商標の悪用もまた最高記録です。

標的にされた産業分野でのその他のカテゴリは、ソーシャルネットワーキングサイトや国税局への攻撃によって全体の4%に達しました。

有害なアプリケーションおよび亜種の総数は、5月に442件で最高記録を出しています。

クライムウェア拡散のURL数は、四半期終わりに爆発的に増加し、2007年第2四半期の終わりより258%増加し、9,529件になりました。

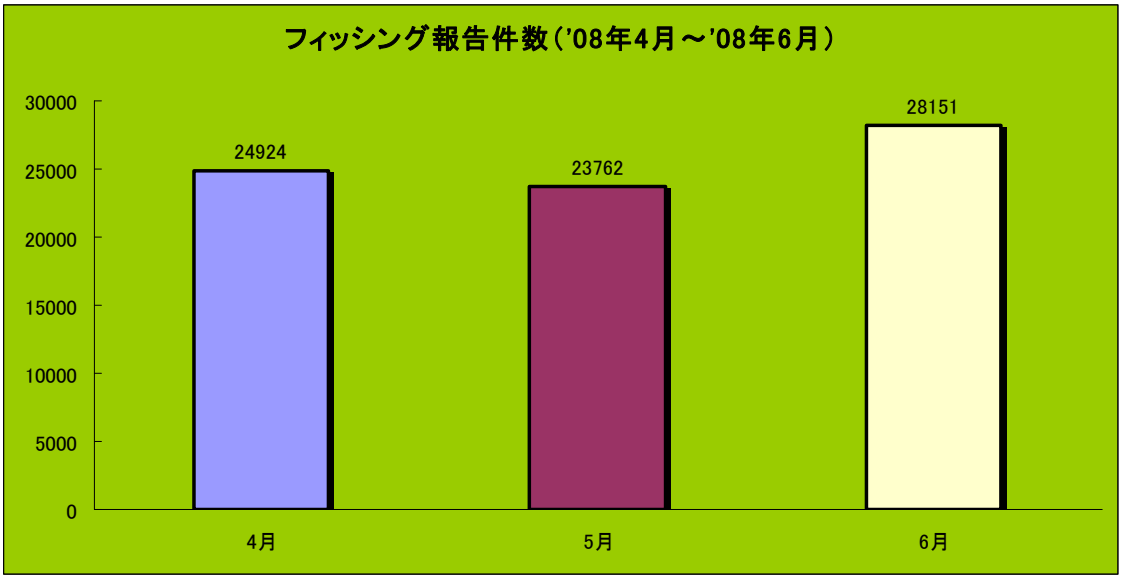
2.【Statical Highlights】統計によるハイライト

表 2.1　フィッシングに関する統計

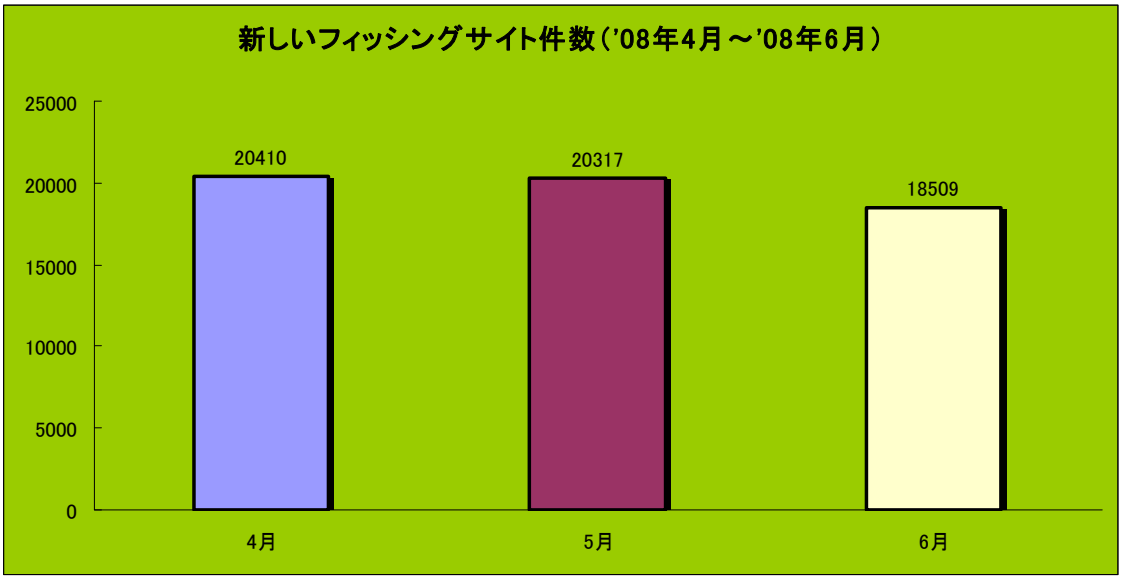
	4 月	5 月	6 月
フィッシングに関する報告件数	24,924	23,762	28,151
報告されたフィッシングサイト数	20,410	20,317	18,509
フィッシングにより乗っ取られた商標数	276	294	227
最も多くのフィッシングサイトをホストした国	中国	トルコ	アメリカ
商標の名前が URL に含まれていた割合	28.3%	23.2%	26.1%
IP アドレスのみでホストネームなしのサイト	5.5%	13.2%	4%
ポート 80 を使用しないサイトの割合	0.81%	0.45%	0.49%
サイトの最長オンライン残存期間	30 日間	31 日間	30 日間

3.【Phishing Email Reports and Phishing Trends】フィッシングメールとフィッシングサイトの傾向

2008 年第 2 四半期のフィッシングに関する報告件数は 5 月に 23,762 件まで減少した後、13%増加し、6 月最後には 28,151 件に達しました。四半期最後の件数は、今年 2 月の記録 30,716 件より 8%低い数で、2007 年 9 月の最高記録 38,514 件に比べると 27%も減少しています。フィッシング報告メールの件数は、一般の方や、APWG メンバー、共同研究者の方々から APWG へ送られてきたものをカウントしています。



2008 年第 2 四半期、APWG によって検知されたフィッシングサイト数は、6 月にわずかな減少を見せ、四半期最初の 4 月に比べると 9%低い 18,509 件検知されました。

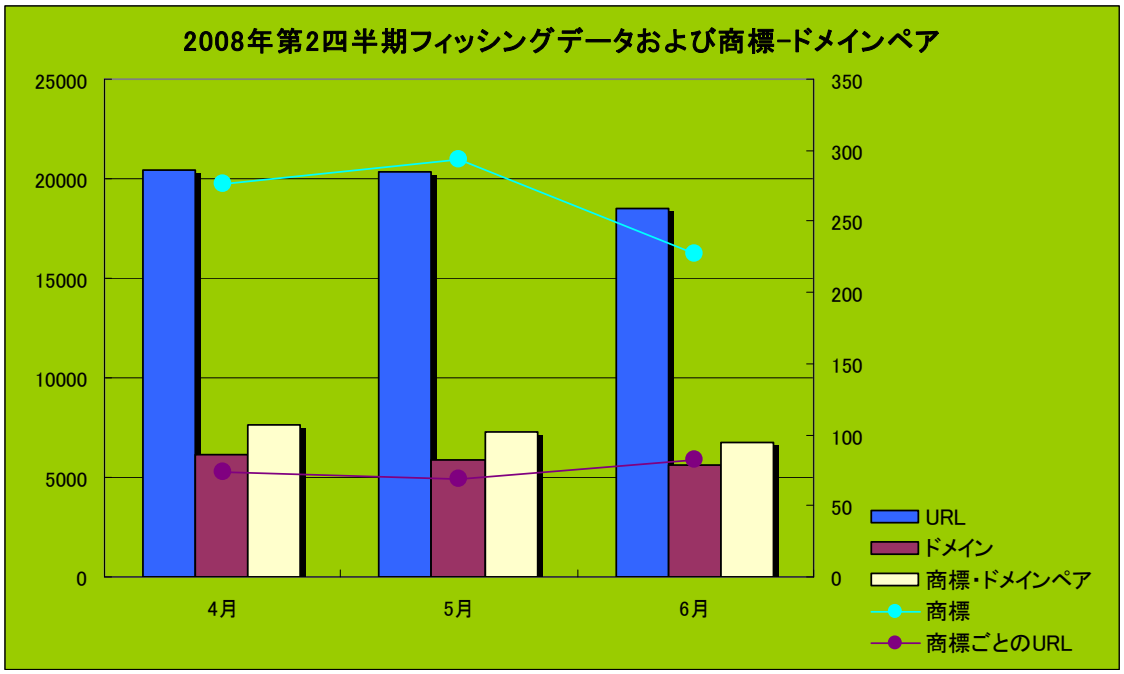


4.【Brand-Domain Pairs Measurement】商標－ドメインペアの観測

次に示す図は、フィッシングされた商標、ドメイン、商標・ドメインのペア、そして URL に基づいた統計値をまとめたものです。商標・ドメインのペアは、特定の商標を標的にするために使用された場合をカウントしています。

※いくつかの URL が同じ商標を標的にしていて、同じドメインにホスティングされている場合、この商標・ドメインのペアは、複数でなく 1 つとしてカウントします。

フォレンジックユーティリティ：フィッシングされた URL の数が、商標・ドメインのペアの数より多い場合、それは多くの URL が同じ商標を標的にするために同じドメインにホスティングされていることを表しています。それぞれのドメインにいくつの URL が対応しているのかを知ることで、攻撃される商標を持つ会社や組織が場所を特定し、無効化する必要があるような攻撃ドメインの概算の数が分かります。また、フィッシング対策技術（ブラウザおよびメールブロッキングなど）は完全な URL を要求するため、ドメインごとに発生した一意な URL の一般的な数を把握することに役立ちます。



商標・ドメインのペアは、4 月から 6 月の調査を通して 7,656 件から 6,768 件へと少しずつ減少しています。これを受けて、MarkMonitor の製品マーケティング部部長の Blake Hayward 氏は、「第 2 四半期中新たなフィッシング URL が減少する一方、標的にされるブランド数は増え続けている」と発言しています。また同氏は、「これはフィッシング犯がさらにスピアフィッシング詐欺を働くために洗練されたマーケティングツールや IT インフラなどに投資していることを示している」と結論付けました。

表 4.1　フィッシングデータに関する表

	4 月	5 月	6 月
URL 数	20,410	20,317	18,509
ドメイン数	6,176	5,849	5,633
商標・ドメインペア数	7,656	7,267	6,768
商標数	276	294	227
商標あたりの URL 数	74	69	82

5.【Most Used Ports Hosting Phishing Data Collection Servers】フィッシングデータをホスティングする収集サーバで最も使用されたポート

2008 年第 2 四半期は、全てのフィッシングサイトで最も HTTP ポート 80 番の使用が多いと報告され、この傾向は APWG が調査、報告を始めてから一貫して続いています。

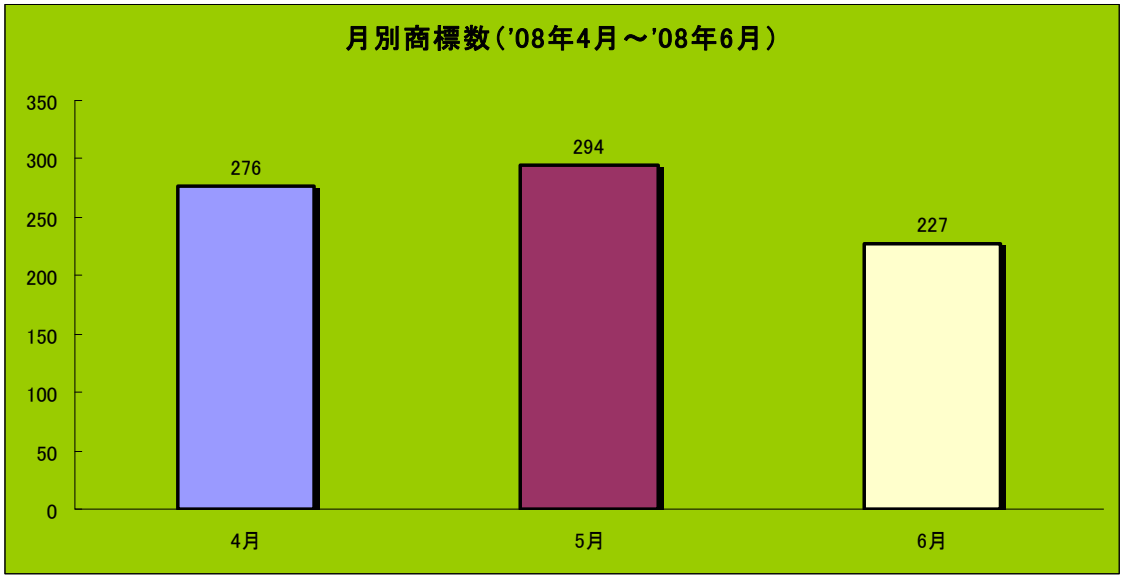
表 5.1　月、ポート別の使用された割合

4 月		5 月		6 月	
ポート 80	99.49%	ポート 80	99.42%	ポート 80	99.65%
ポート 5443	0.23%	ポート 82	0.16%	ポート 443	0.19%
ポート 443	0.22%	ポート 84	0.06%	ポート 84	0.06%
ポート 8080	0.06%	ポート 85	0.06%	ポート 81	0.03%
		ポート 443	0.06%	ポート 9070	0.03%
		その他 5 つ	0.24%	その他 1 つ	0.01%

6.【Brand and Legitimate Entities Hijacked by Email Phishing Attacks】メールフィッシング攻撃によって乗っ取られた商標および正規の組織等

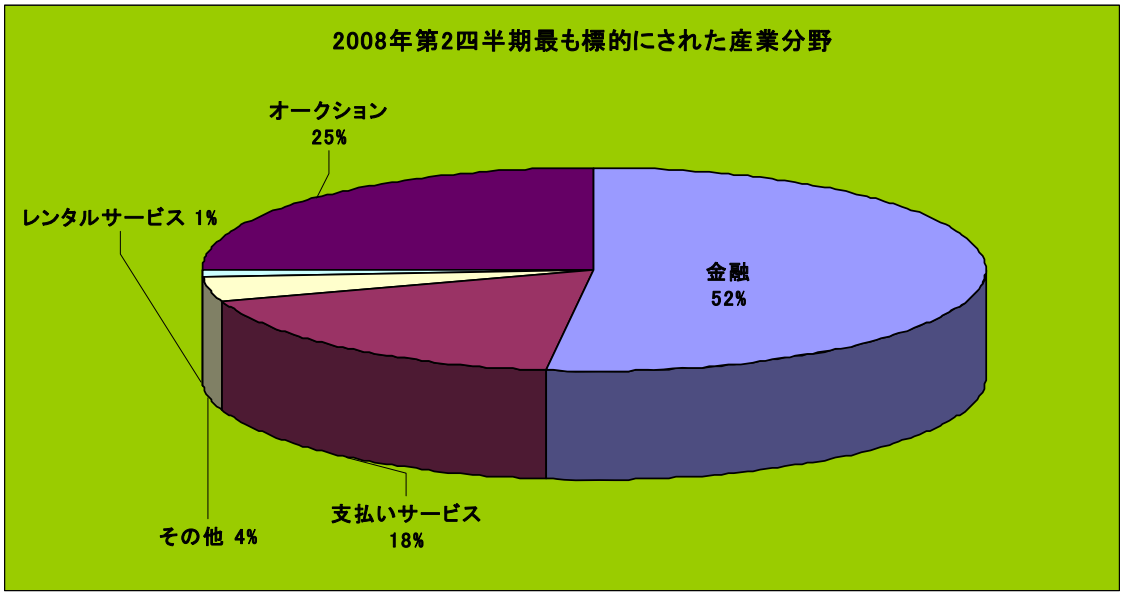
2008 年第 2 四半期､期間中乗っ取られた商標の数は 276 件から 227 件と 28%の減少を見せました。このデータセットで、5 月は 294 件で最高値を記録しており、四半期を通した 485 件もまた最高記録となっています。

.



7.【Most Targeted Industry Sectors】最も標的にされた産業分野

2008 年第 2 四半期は、引き続き金融関連サービスが最も標的にされた産業分野になりました。これは APWG が標的にされた産業分野の調査を始めてからは変わっていません。“その他”の項目の上昇は、MySpace および Facebook のようなソーシャルネットワーキングサイトや国税局への攻撃の増加による影響だと思われます。5 月および 6 月はまた、携帯電話プロバイダおよび製造業へ向けた大規模な攻撃の増加が見られました。



8.【Countries Hosting Phishing Sites】フィッシングサイトをホスティングしている国

5 月中、トルコが最も多くのフィッシングサイトをホスティングしている国として 1 位になりました。この上昇は、けた外れに多くのフィッシング攻撃を受けた ISP によるものと思われます。IP アドレス空間を悪用しているハッカーが、その ISP に多くのフィッシング詐欺サイトをホスティングしました。アメリカは、期間中常に上位 2 国内にとどまり 6 月には再び 1 位になっています。中国は、前の 3 月に上位国のうちたった 3%しかホスティングしていなかった状態から 4 月には急激な増加を見せました。

表 8.1 国別フィッシングサイトホスト率

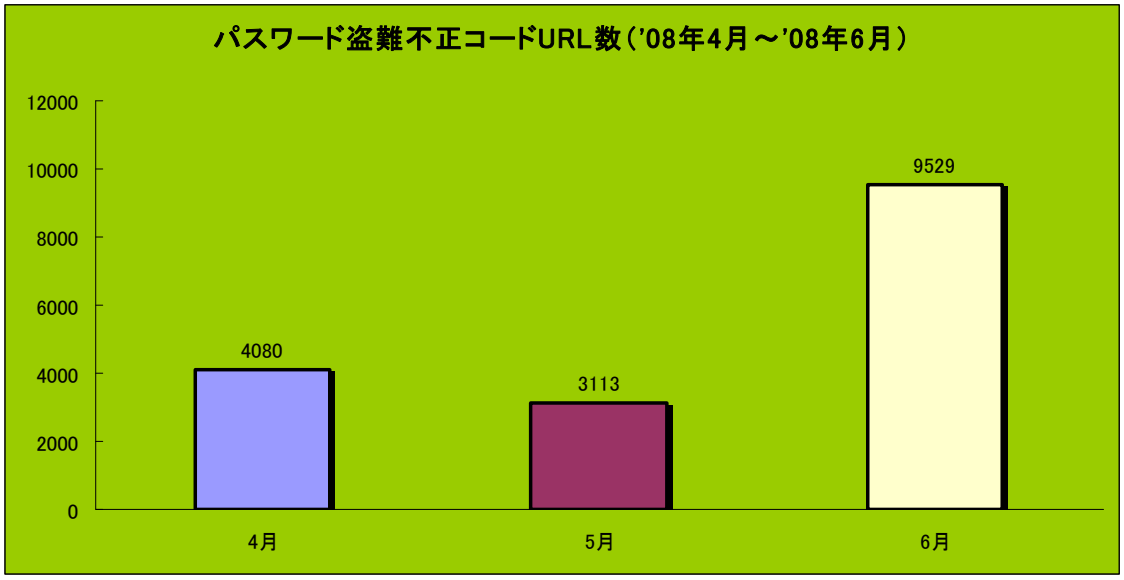
4 月		5 月		6 月	
中国	25.19%	トルコ	25.73%	アメリカ	18.93%
アメリカ	16.68%	アメリカ	17.16%	トルコ	17.92%
ロシア	8.23%	日本	11.23%	ポーランド	13.56%
ポーランド	7.15%	中国	9.17%	ギリシャ	6.86%

トルコ	5.79%	ポーランド	7.41%	中国	5.87%
ドイツ	3.97%	ロシア	3.27%	ロシア	4.28%
韓国	3.12%	ギリシャ	2.11%	フランス	2.48%
ギリシャ	2.61%	フランス	2.08%	韓国	2.38%
フランス	2.32%	韓国	1.60%	ブルガリア	2.28%
ルーマニア	2.21%	オランダ	1.60%	イギリス	2.16%

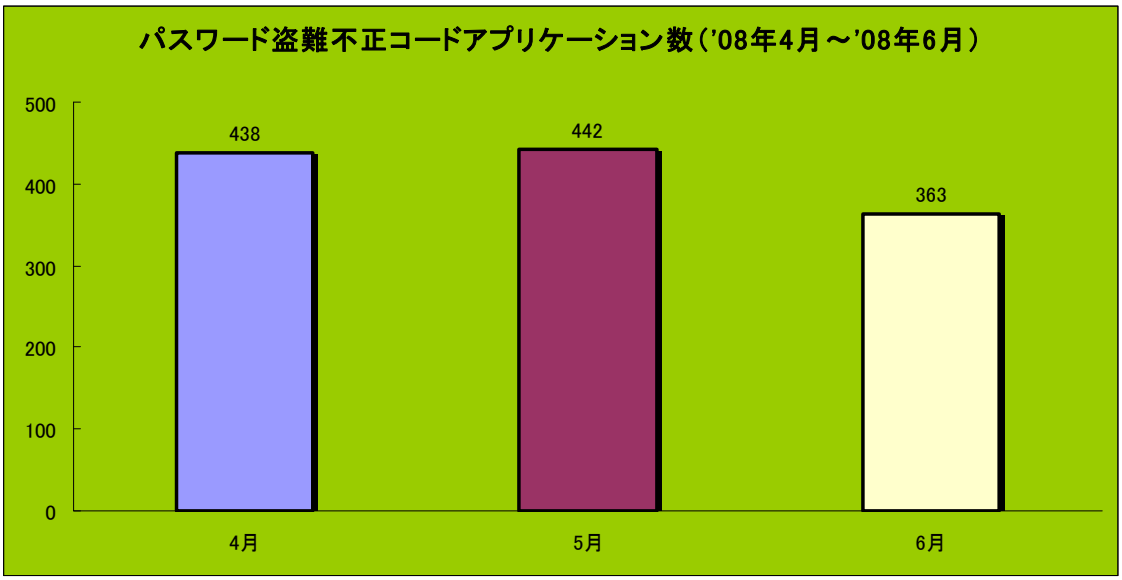
9.【Phishing-based Trojans-keyloggers】フィッシングベースのトロイの木馬およびキーロガー

クライムウェアを広める URL の数は、4 月の 4,080 件から、6 月の 9,529 件まで増加が見られました。この上昇は、3 月の 6,500 件より約 47%の増加で、また今四半期終わりの 6 月の件数は 2007 年の第 2 四半期終わりに比べ 258%もの増加となっています。

Websense 主任技術員であり、本レポートのアナリストである Dan Hubbard 氏は、「この大幅な上昇は SQL インジェクション攻撃に使用される悪意のあるコードが原因ではないか」と発言しています。



キーロガーおよびクライムウェア指向の有害アプリケーションの数は、常に高いレベルを保っており、5 月には、216 件の有害なアプリケーションが検知された 2007 年 5 月より 105%多く、また前月より 1%増加して 442 件を記録しました。結果からハッカーたちは、明らかに企業やその消費者のセキュリティ対策をすり抜けるための新技術開発を行っていると思われます。



・フィッシングベース　トロイの木馬－リダイレクタ

定義：エンドユーザーを本来意図されていないネットワーク上の場所に誘い出すことを目的として設計されたクライムウェアのコード。これにはホストファイルや他の DNS 特有の情報を改ざんするようなクライムウェア、詐欺サイトへ情報を誘導するようなブラウザー・ヘルパー、詐欺地点への誘導を行うネットワーク・レベルでのドライバやフィルターのインストールを行うクライムウェアを含みます。これらは全て個人情報の盗難やその他の信用情報の不正取得という犯罪目的のためにインストールされます。

フィッシング用キーロガーの使用と共に、情報の行先を変えてしまうトラフィックリダイレクタの使用も顕著に増加しているようです。特に、単純にユーザ PC の DNS サーバやホストファイルのセッティングを部分的に変更することにより、特定の、あるいは全ての DNS ルックアップを詐欺用の DNS サーバに再誘導（リダイレクト）するという不正コードの使用が最も多く見受けられます。詐欺用サーバはほとんどのドメインに対して有効なレスポンスを応答します。しかしながら、フィッシング犯達が消費者を銀行のサイトに似せた詐欺用サイトに誘導したいと考えた場合、単にネーム・サーバーの応答をその特定のドメイン向けに変更します。これはフィッシング犯達がユーザ側からのいつどのような入力操作についても、ユーザにこのような不正な行為が行われていることを知られることなくリダイレクトするための特に有効な手段と考えられます。ユーザが自分で目的のサイトのアドレスを打ち込み、メール本文や「インスタントメッセージ」中のリンク先に入るという行為を行わなかったとしてもフィッシングに巻き込まれてしまうのです。

10.【Phishing-based Trojans and Downloader's Host Countries(by IP address)】IP アドレスによるトロイの木馬およびキーロガーのダウンローダホスト国

以下の表は本四半期、フィッシング用キーロガーもしくはキーロガーのダウンローダのいずれかの形で有害なコードをホスティングしているとして分類されたウェブサイトの調査結果です。

表 10.1 トロイの木馬およびキーロガーのダウンローダホスト国分類

4 月		5 月		6 月	
アメリカ	38.67%	アメリカ	32.12%	アメリカ	30.98%
中国	9.68%	中国	28.67%	中国	24.95%
ロシア	8.23%	ロシア	6.06%	イタリア	13.34%
ドイツ	4.10%	ブラジル	4.71%	ロシア	5.74%
韓国	3.81%	フランス	3.10%	ドイツ	2.56%
カナダ	2.86%	ドイツ	2.91%	ブラジル	2.45%
フランス	2.46%	オランダ	2.45%	韓国	2.17%
イタリア	1.96%	韓国	2.18%	フランス	1.99%
ルーマニア	1.59%	カナダ	1.61%	カナダ	1.79%
ポーランド	1.52%	イタリア	1.46%	イギリス	1.75%

11.【APWG Phishing Trends Report Contributors】APWG Phishing Trends Report 協力事業者

・MarkMonitor

MarkMonitor は、オンライン決済などに対してする安全に特化した統合的オンライン個人情報プロテクションサービスを提供する国際リーダー企業です。

・PandaSecurity

PandaSecurity は、ユーザをマルウェアから守ることに特化した研究と技術サポートセンターの国際ネットワーク企業です。

・Websense

Websense Security ラボの目的は、コンピュータ環境で働く従業員を脅かす進化するインターネットの脅威に関する発見、調査、報告です。

Phishing Attack Trends Report は、APWG によって四半期毎に発行され、フィッシング、クライムウェア、メール盗聴の問題増加によって引き起こされる個人情報の盗難や詐欺の撲滅に焦点を当てた産業および司法当局などの団体から成ります。より詳しい情報についてはこちらのいずれかへ連絡して下さい、APWG Deputy Secretary General Foy Shiver 404.434.7282、Cas Purdy 858.320.9493、cpurdy@websense.com、TeSmith 831.818.1267、Te.Smith@markmonitor.com。

APWG は、このレポートでのデータ、分析について全ての上記協力メンバーに感謝します。

・APWG について

APWG（フィッシング対策ワーキンググループ）は、顕著になりつつあるフィッシングやメールスプーフィングの問題に起因する個人情報の窃盗および詐欺行為の撲滅対策を中心として活動する連合団体です。この連合団体は、フィッシング問題について討議し、ハードおよびソフトのコスト面からフィッシング問題の範囲を定義し、問題解決のための情報と最良の実践例を共有するためのフォーラムを提供します。また、適当と判断される場合には、APWG はこれらの情報を司法当局と共有する場合があります。

APWG には 1,800 以上の企業および政府機関が加入しており、会員数は 3,200 名以上に上ります。フィッシング攻撃およびメール詐欺は、オンライン上でビジネスを行う多くの組織にとって機密にかかわる問題であるため、APWG の方針として会員組織についての情報は公開していません。グループへの加入は、一定条件を満たす金融機関、オンライン小売業者、インターネットサービスプロバイダ（ISP）と司法機関およびソリューション・プロバイダーに公開しています。

APWG はタンブルウィード・コミュニケーションズおよび数社の会員銀行と金融機関、Ｅコマースプロバイダによって設立されました。2003 年 11 月にサンフランシスコにおいて最初の会合が開かれ、その後 2004 年 6 月には、グループの運営委員会と理事会および執行委員会により運営が管理される独立法人となりました。